Informatieveiligheid

Informatieveiligheidsbeleid Provincie Zeeland 2023 - 2026

Provincie Zeeland

Informatie Veiligheid

Informatieveiligheidsbeleid Provincie Zeeland 2023 – 2026

Datum	10 augustus 2023
Auteur	CISO Provincie Zeeland
Versienummer	2.0
Classificatie	Openbaar

Inhoudsopgave

1. Inleiding

1.1. Aanleiding en belang

De Provincie Zeeland is in toenemende mate afhankelijk van de beschikbaarheid van betrouwbare informatie en informatievoorziening. Dit is onder meer het gevolg van de steeds verdergaande digitalisering en ketenintegratie binnen de publieke sector. Uit het Cybersecuritybeeld 2020 van het Nationaal Cyber Security Centrum (NCSC) blijkt dat kwaadwillenden zich ook richten op overheden, niet alleen voor spionage maar ook voor informatiemanipulatie en sabotage. Door deze ontwikkelingen kunnen nieuwe kwetsbaarheden aan het licht komen en risico's ontstaan. Daarnaast is nog steeds de mens de zwakste schakel bij informatieveiligheid: veel incidenten komen voort uit onopzettelijke fouten, vaak uitgelokt door social engineering.

Onder informatieveiligheid wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen. Deze kwaliteitsaspecten zijn van oudsher de pijlers van informatieveiligheid. Aanvullend heeft de Provincie Zeeland privacy als vierde kwaliteitsaspect toegevoegd. Hierbij gaat het ook om het borgen van de effectiviteit van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

Informatieveiligheid is een beleidsverantwoordelijkheid van de provinciale organisatie als geheel, en is primair belegd bij Gedeputeerde Staten. Immers, onvoldoende informatieveiligheid kan leiden tot onacceptabele risico's voor het bedrijfsproces van de Provincie. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

Informatieveiligheid zelf is géén primair of secundair proces, géén kerntaak, maar als je er niets aan doet gaat het wel ten koste van de kerntaken van de organisatie: informatieveiligheid op orde is een randvoorwaarde voor een efficiënt en effectief primair proces.

De Provincie Zeeland heeft de ambitie om met het onderhavige beleidsdocument de informatieveiligheid structureel naar het BBN2 niveau van de Baseline Informatieveiligheid Overheden (BIO) te brengen. Dit niveau wordt geborgd door het opstellen, implementeren en in stand houden van een managementsysteem (ISMS) op basis van ISO27001 (Gecertificeerd op 26 januari 2023).

1.2. Doel

Het doel van dit beleid is het (opnieuw) vaststellen van de organisatie van en de uitgangspunten voor de beheersing van informatieveiligheid binnen de Provincie Zeeland. Het legt daarmee een basis voor:

- Het waarborgen van de veiligheid van de informatie die de Provincie verwerkt.
- Het waarborgen van de privacy van zowel burgers als medewerkers.
- Een betrouwbare bedrijfsvoering via een betrouwbare informatievoorziening.
- Het kader waarbinnen informatieveiligheid binnen de Provincie georganiseerd wordt.

Dit beleid is de richtlijn voor alle medewerkers en bestuur om veilig met informatie om te gaan. Het geeft de keuzes aan die door de Provincie Zeeland zijn gemaakt. Het beschrijft basisprincipes, verantwoordelijkheden, aanpak en rapportagelijnen.

Dit beleid is in overeenstemming met de eisen uit de ISO 27001/27002 norm voor informatieveiligheid en de Baseline Informatieveiligheid Overheid (BIO).

In dit document wordt vooral de term *informatieveiligheid* gebruikt in plaats van *informatiebeveiliging*. De reden hiervoor is dat over het algemeen informatiebeveiliging een defensief en technisch karakter kent. Dit doet geen recht aan het onderwerp, waarvan de essentie is 'het veiligstellen' van informatie. Dit gebeurt net zo goed door zorgvuldig handelen in het gebruik ervan als door technische maatregelen.

Het informatieveiligheidsbeleid is afgeleid van de provinciale informatiestrategie en maakt onderdeel uit van het informatiebeleid (zie bijlage 1 voor de samenhang tussen de verschillende beleidsstukken).

Het *proces* (Plan-Do-Check-Act (PDCA) cyclus) rond de beheersing van informatieveiligheid is verder uitgewerkt in het document 'Managementproces voor informatieveiligheid'. Daarnaast wordt dit beleid ondersteund door diverse beleidsdocumenten en operationele procesbeschrijvingen.

1.3. Gerelateerde documenten

Informatieveiligheid is een dynamisch proces. Dit is het gevolg van voortdurende organisatorische, juridische en technologische veranderingen. Op basis van dit algemeen beleidskader worden specifieke organisatie eigen richtlijnen en beheersmaatregelen per categorie uitgewerkt. De belangrijkste zijn hieronder opgesomd. De Chief Information Security Officer (CISO) is verantwoordelijk voor het voorstellen van wijzigingen of aanvullingen. Tevens zorgt hij voor het inbrengen van deze zaken in de betreffende management overleggen. Zie ook de bijlage 1.

- Informatiebeleidskader Provincie Zeeland 2020-2023
- Managementproces voor informatieveiligheid
- Beleid Logische Toegangsbeveiliging
- Beleid Cryptografie
- Beleid Mobiel Werken
- Beleid Infrastructuur
- Beleid Beheer Middelen
- Standaarddiensten ICT
- Standaarddiensten PO
- Standaarddiensten FAC

1.4. Doelgroep

De doelgroep van dit document omvat alle medewerkers van de provincie Zeeland, vast en tijdelijk, intern en extern. Vanwege de brede relevantie is het document voor iedereen beschikbaar op Start.

1.5. Beheer van dit document

Dit beleid wordt vastgesteld door het college van Gedeputeerde Staten (GS) en eigendom van de afdelingsmanager IA. Deze is tevens Chief Information Officer (CIO) en is door de directie aangewezen als verantwoordelijke voor Informatieveiligheid.

De geldigheid van dit document is vastgesteld op 4 jaar vanaf de datum van inwerkingtreding. Daarna wordt jaarlijks, of wanneer ontwikkelingen daarom vragen, door de CISO een evaluatie uitgevoerd om na te gaan of dit document nog een juiste weergave is van het managementproces.
Deze tussenversies worden vastgesteld door de CIO en krijgen een volgnummer.

Versie	Datum	Opmerking
1.0	1-10-2019	**Definitieve versie, vastgesteld door GS voor 4 jaar.**
1.1	15-12-2020	Geactualiseerde versie 2020 nav verdere inrichting van ISMS
1.2	15-6-2021	Geactualiseerde versie 2021
1.3	7-2-2022	Aanpassingen n.a.v. interne audits
1.4	1-8-2022	Aanpassingen onderdeel Wet- en Regelgeving door jurist
1.5	10-11-2022	Aanpassing van de scope (reikwijdte) en de locatie n.a.v. 1e Fase audit. Daarmee ook bij de belanghebbenden van de context (2.4) de verhoudingen tussen IA en de organisatie aangegeven.
2.0	10-08-2023	**Definitieve versie, vastgesteld door GS voor 4 jaar.**

2. Informatieveiligheid

2.1. Visie op informatieveiligheid

Informatie is één van de voornaamste bedrijfsmiddelen van de Provincie Zeeland. Het verlies van gegevens en informatie, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties.

Betrouwbare en veilige informatieverwerking is dan ook zeer belangrijk, evenals de integriteit en beschikbaarheid van informatie. De Provincie Zeeland heeft een aantal strategische uitgangspunten vastgesteld om de veiligheid van informatie richting te geven. Deze uitgangspunten zijn vastgelegd in dit beleid. Het document is bindend voor alle (externe) medewerkers en leveranciers van de Provincie Zeeland.

De Provincie Zeeland is zich er daarbij van bewust dat informatieveiligheid meer behelst dan uitsluitend technische maatregelen, waar vaak als eerste aan gedacht wordt. Zorgvuldig omgaan met informatie is evenzeer een zaak van bewustwording door alle medewerkers en het afstemmen van de eigen werkwijze hierop.

In de planperiode van dit document zet de Provincie Zeeland in op het verbreden van informatieveiligheid en het verder verhogen van de bewustwording bij medewerkers, directie, bestuur en statenleden. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de organisatie. Informatieveiligheid vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn; ieder organisatieonderdeel is hierbij betrokken. Tevens is het van belang het behaalde ISO-27001-certficaat te behouden.

2.2. Reikwijdte

Dit beleid heeft betrekking op de informatievoorziening van de interne organisatie van de Provincie, zowel kantoor- als procesautomatisering, van de Provincie Zeeland inclusief de werkomgeving van het provinciaal bestuur (Commissaris van de Koning en Gedeputeerde Staten), de internetomgeving, mobiele apparaten en thuiswerkvoorzieningen. Het beleid heeft ook betrekking op informatie in bijvoorbeeld papieren dossiers, mobiele computers, USB-sticks, smartphones, tablets en dergelijke. De geautomatiseerde gegevensuitwisseling met externe organisaties, informatiesystemen in beheer bij derde partijen en de ontwikkeling van informatiesystemen vallen ook binnen de scope van dit beleid.

Het informatieveiligheidsbeleid dient door medewerkers van alle organisatieonderdelen te worden opgevolgd, ongeacht de locatie waar men werkt. Dit is inclusief de telewerkplek.

Het managementsysteem voor Informatieveiligheid (het ISMS) dat door de provincie ingericht is omvat de aanschaf, exploitatie en beheer van de kritische applicaties, ICT-voorzieningen en ICT-infrastructuren.

Om deze doelen te bereiken worden door de provincie de volgende processen en activiteiten uitgevoerd, al dan niet uitbesteed (belangrijkste processen):

- Visie- en beleidsvorming
- Projecten en programma's
- Informatievoorziening aan burgers en bedrijven
- Vergunningverlening
- Subsidieverlening
- Handhaving
- Beheer en exploitatie van infrastructurele voorzieningen

Daarnaast geldt het ISMS voor de interne, ondersteunende processen van de provincie Zeeland: HR, ICT, Facilitaire diensten, Financiën, Juridische zaken, Inkoop en contractmanagement.

De geografische scope van het ISMS bestaat uit de hoofdlocatie van de provincie Zeeland:

- Kantoorcomplex Abdij 6 Middelburg.

2.3. Context: ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatieveiligheidsbeleid zijn de volgende:

Interprovinciale Digitale Agenda
Provincies werken in gezamenlijkheid aan de Interprovinciale Digitale Agenda (IDA) met daarin verschillende sporen: innovatie, data, dienstverlening en bedrijfsvoering. Samenwerking staat daarbij centraal. Daarnaast wordt aangesloten op de digitale agenda's van andere bestuurslagen waarmee wordt samengewerkt. De digitale transformatie, die in de gehele maatschappij gaande is, biedt kansen maar levert tegelijkertijd ook risico's op die onderkend moeten worden. De Provincie moet enerzijds in staat zijn om informatie adequaat te kunnen delen met keten- en netwerkpartners en anderzijds hierbij kritisch te zijn in relatie tot informatieveiligheid.

Nieuwe wetgeving: Wet Open Overheid, Wet Elektronische Bekendmakingen, de Omgevingswet en de Netwerk Informatiebeveiligingsrichtlijn (NIB/NIS2)
De Wet Open Overheid vraagt een open en transparante informatievoorziening, zowel intern als extern (vindbaar, uitwisselbaar, eenvoudig te ontsluiten en goed te archiveren). De Wet Elektronische Bekendmakingen richt zich op het volledig elektronisch bekendmaken van publicaties. De Omgevingswet zal een impuls geven om de organisatie meer integraal te laten werken. Er worden twee belangrijke onderdelen onderscheiden, namelijk het Digitaal stelstel Omgevingswet en diverse informatieproducten die eventueel in een later stadium zullen worden ontsloten via zogenaamde informatiehuizen. De NIS2-richtlijn richt zich op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. De komst van de richtlijn moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties.

Samenwerking
De Provincie werkt in toenemende mate samen met verschillende (keten)partners. Uitwisseling van informatie in verschillende vormen is daarbij een onlosmakelijk onderdeel. In dit kader worden ook gezamenlijk met partners of zelfstandig informatieproducten ontwikkeld, waarbij het gebruik van (cloud)diensten van derden toeneemt. Verder wordt op interprovinciaal niveau samenwerking gezocht op het gebied van data en applicaties (GBO). Tenslotte zijn er initiatieven om op het gebied van ICT dienstverlening (kantoorautomatisering) samen te werken met één of een aantal regionale partners. Voor beide vormen van samenwerking is het van belang dat informatieveiligheid een integraal onderdeel vormt van de werkwijze en te maken afspraken daarover.
Om die samenwerking te bevorderen is in 2023 in het kader van de Zeeuwse Norm Weerbare Overheid de Zeeuwse CISO-kring opgericht waar alle CISO's van provincie, gemeenten, waterschap, GGD, Veiligheidsregio, Zeeuws Archief, Orionis deel van uitmaken en onderling informatie delen.
Daarnaast is er op interprovinciaal niveau het CIBO (Centraal Informatie Beveiligingsoverleg) waarin alle CISO's van de 12 provincies en BIJ12 zitting hebben en het IP-ISAC (Interprovinciaal Information Sharing Analysis Center) waarin alle provinciale technische securityspecialisten zitting hebben.

Cloud beleid
In algemene zin is er een ontwikkeling in gang gezet waarbij een toenemend aantal informatiesystemen via SAAS (software as a service) oplossingen worden afgenomen van leveranciers, de Provincie anticipeert hierop al een aantal jaren bij nieuwe ontwikkelingen. Dit impliceert dat een deel van de informatie op andere locaties is opgeslagen dan de serverruimten binnen de Abdij en het Waterschapsgebouw. Het is van belang dat er passende afspraken gemaakt worden met leveranciers ten aanzien van betrouwbaarheid, integriteit en vertrouwelijkheid van deze informatie en dat op naleving hiervan ook wordt toegezien.

Baseline Informatieveiligheid Overheden (BIO)
Overheden hebben onderling afgesproken dat zij met ingang van 1 januari 2020 voldoen aan de maatregelen zoals omschreven in de baseline informatieveiligheid overheden (BIO). Deze baseline is gebaseerd op de maatregelen uit ISO27002. Sinds 26 januari 2023 is Provincie Zeeland gecertificeerd op de ISO 27001/2 en voldoet ook aan de maatregelen van de BIO.

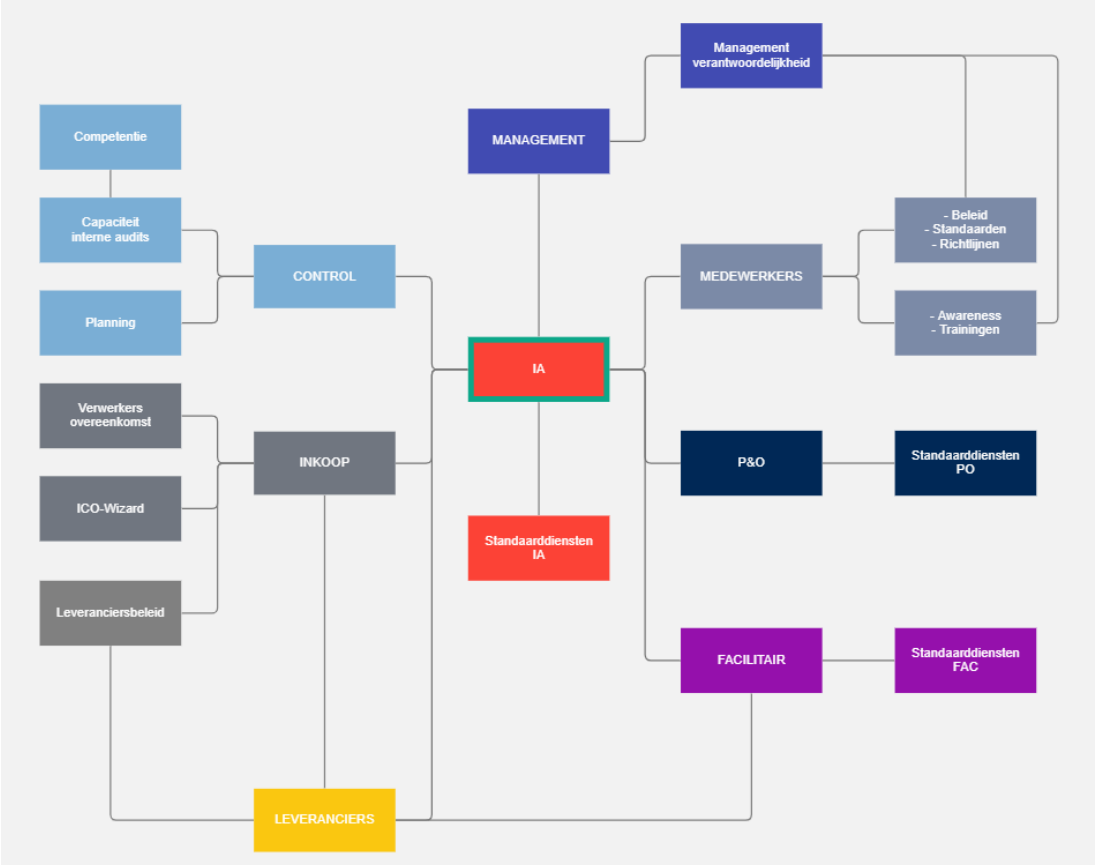
2.4. Context: belanghebbenden

De provincie heeft meerdere interne en externe belanghebbenden, waarvoor een goede informatieveiligheid direct relevant is.

De interne belangen bestaan voornamelijk uit het garanderen van een passend en effectief niveau van informatieveiligheid, waarbij de vertrouwelijkheid rond persoonsgegevens in de provinciale applicaties een extra nadruk heeft. De provincie komt hieraan tegemoet door het conformeren aan de ISO27001 en het implementeren van de AVG. Het inrichten van een PDCA cyclus zorgt ervoor dat informatieveiligheid ook passend en effectief blijft. Door het definiëren van een standaardniveau van beveiligingsmaatregelen en het uitvoeren van gerichte risicoanalyses worden specifieke belangen en behoeften geïdentificeerd, zodat maatwerk mogelijk is.

De belangen van externe partijen worden, voor zover die niet al door bovenstaande uitgangspunten worden geborgd, gediend door het naleven van betreffende wet- en regelgeving, die voor die specifieke partij of situatie geldt. Ook hier zorgt het instrument van risicoanalyse voor de identificatie van specifieke wensen en eisen en maatwerk.

Inzoomend op de interne belanghebbenden wordt hieronder in schema weergegeven hoe afdeling I&A zich verhoudt tot de rest van de organisatie in het kader van de dienstverlening op het gebied van ISO 27001:



2.5. Wet- en regelgeving

Bij het opstellen van dit beleid is rekening gehouden met de eisen die gesteld worden in de onderstaande wet- en regelgeving. Dit overzicht wordt getoetst bij de periodieke herziening van dit beleidsdocument.

Wet- en regelgeving	Effect wet- en regelgeving op informatievoorziening provincie
ISO27001	Aantoonbaar voldoen aan de normen uit de ISO27001 norm in de vorm van een certificering. De aantoonbaarheid is vastgelegd in het ISMS (Strict Control Cockpit).
Baseline Informatieveiligheid Overheid (BIO)	Aantoonbaar voldoen aan de normen uit de BIO als afgeleide van de eisen uit de ISO27001. De aantoonbaarheid is vastgelegd in het ISMS.
Algemene verordening gegevensbescherming (AVG)	De provincie heeft de verplichtingen die voortvloeien uit de AVG, waaronder verplichtingen met betrekking tot informatiebeveiliging, geïmplementeerd in de organisatie. Het opstellen van diverse documentatie (bijvoorbeeld privacybeleid, privacyreglementen en verwerkingsregister) en procedures (bijvoorbeeld voor de rechten van betrokkene) heeft ervoor gezorgd dat de basis voor de naleving van de AVG, waaronder de governance, op orde is.
Meldplicht datalekken (uit de AVG)	De meldplicht beschrijft dat organisaties zo snel mogelijk (binnen 72 uur) een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een (ernstig) datalek hebben. De provincie meldt datalekken bij de Autoriteit Persoonsgegevens als het gaat om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is. Tevens meldt de provincie het datalek aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene.
Wettelijke bewaartermijnen	De provincie houdt zich aan de wettelijke voorschriften ten aanzien van bewaartermijnen, zoals die bijvoorbeeld in de Archiefwet zijn vastgelegd. Dit betreft alle informatie zoals die bijvoorbeeld is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e-mail. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.
Wet computercriminaliteit	Indien er aanvallen op de provincie plaatsvinden die die beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal de provincie in beginsel aangifte doen. De CISO adviseert hierover aan de CIO en directie – alleen de directie kan het besluit tot aangifte nemen. Als er een melding gedaan wordt van een zwakke plek in de systemen van de provincie en daarbij het responsible disclosure beleid wordt gevolgd, neemt de provincie geen juridische stappen tegen de melder. Het Openbaar Ministerie heeft altijd het recht om zelf te beslissen of het strafrechtelijk vervolgt. De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De relevante artikelen zijn gericht op: • Vernieling, beschadigen en onbruikbaar maken van een systeem; • Aftappen van gegevens; • DoS-aanvallen (Denial of service); • Computervredebreuk; • Diensten afnemen zonder betalen; • Malware en kwaadaardige software.
Standaarden Forum voor Standaardisatie	De provincie hanteert bij de inrichting de standaarden en past het ‘pas toe of leg uit’ principe toe.
Wet open overheid	Vanuit de Wet open overheid zal er steeds meer vanuit eigen beweging informatie openbaar gemaakt moeten worden. Deze wet vraagt met name extra aandacht voor dataclassificatie binnen de informatievoorziening van de provincie. Hieronder valt ook het inregelen van autorisatie, rollen en rechten.

Wet elektronische publicaties	Deze wet verplicht de provincie om alle wettelijk voorgeschreven bekendmakingen, mededelingen en kennisgevingen van besluiten en beleidsregels te publiceren op www.officielebekendmakingen.nl.
Wet modernisering elektronisch bestuurlijk verkeer (inwerkingtreding naar verwachting per 01-01-2023)	Met de wet krijgen inwoners en ondernemers recht om op digitale wijze in contact te treden met de provincie. Dit betekent onder andere dat de provincie verplicht is om voor ieder formeel bericht aan de provincie (denk aan aanvragen voor subsidies of vergunningen, zienswijzen en bezwaarschriften) digitale kanalen open te stellen voor burgers en bedrijven. Deze wet vraagt specifieke aandacht op het gebied van beveiliging van de informatie-uitwisseling. Mogelijk is een heroriëntatie nodig op het gebied van autorisatie, taken en bevoegdheden .
Wet digitale overheid (Wdo) (inwerkingtreding mogelijk per 01-01-2023)	Met deze kaderwet worden een aantal generieke bouwstenen in het digitaal zaken doen met de provincie geregeld (authenticatie, toegankelijkheid, standaarden e.a.). De Wdo geeft onder andere ook uitwerking aan de Europese eIDAS verordening. Deze wet vraagt specifieke aandacht op het gebied van beveiliging van de informatie-uitwisseling. Mogelijk is een heroriëntatie nodig op het gebied van autorisatie, taken en bevoegdheden .
Omgevingswet	De Omgevingswet vraagt specifieke aandacht op het gebied van informatie-uitwisseling (met het DSO en met ketenpartners). Daarnaast ontstaat een nieuw Omgevingswet-applicatielandschap. Bij de aanschaf en implementatie van nieuwe applicaties verdient informatiebeveiliging specifieke aandacht. Tevens heeft de implementatie van de Omgevingswet mogelijk implicaties voor de wijze van besluitvorming en publicatie. Voor de bijbehorende processen is mogelijk een heroriëntatie nodig op het gebied van autorisatie, taken en bevoegdheden. In de interprovinciaal ontwikkelde referentiearchitectuur zijn de aandachtgebieden op het gebied van informatieveiligheid benoemd.
NIS-2 (Netwerk Informatiebeveiligingsrichtlijn)	De NIS2-richtlijn richt zich op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. De komst van de richtlijn moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties. De NIS2 is de opvolger van de eerste NIS-richtlijn, ook wel bekend als de NIB, die in Nederland in 2016 is opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Deze wet wordt nu hoogstwaarschijnlijk ook verplicht voor lokale overheden, maar e.e.a. is nog onduidelijk. De Kamer heeft op 6 juli 2023 unaniem een motie (Slootweg) aangenomen waarin om duidelijkheid gevraagd wordt en uitstel van de uitvoering tot 1-1-2025. De minister gaf deze motie oordeel Kamer.

Verder bestaat het wettelijk kader meer algemeen uit: de Grondwet, de Ambtenarenwet en de Collectieve Arbeidsvoorwaardenregeling Provincies (CAP) en de opvolger CAO Provinciale sector.

3. Uitgangspunten

3.1. Algemeen

De Provincie Zeeland hanteert een kader voor de inrichting en verdere uitwerking van informatieveiligheid. Deze zijn ook deels opgenomen in het Informatiebeleid van de provincie. De onderstaande uitgangspunten worden daarbij gehanteerd. Dit kader dient als leidraad wanneer er zich vraagstukken voordoen op het gebied van informatieveiligheid die niet nog verder zijn uitgewerkt.

1. Veilig omgaan met informatie is een **verantwoordelijkheid van alle medewerkers** in de hele organisatie. Bij een eventuele schending van één of meer verplichtingen uit het Informatieveiligheidsbeleid, kan de betreffende medewerker daarop worden aangesproken door zijn direct leidinggevende, en afhankelijk van de aard en de mogelijke gevolgen van de schending, worden geconfronteerd met een personele beslissing.
2. **Het management is primair verantwoordelijk** voor de invoering en handhaving van informatieveiligheid binnen de onderscheiden organisatie onderdelen en stelt medewerkers in staat hun verantwoordelijkheid te nemen.
3. Ieder proces, informatiesysteem, gegeven en generieke infrastructuur (fysiek en informatie) heeft één **formele eigenaar** op managementniveau.
4. De Provincie heeft een aantal **standaard maatregelen** getroffen, waarmee een basisniveau voor informatieveiligheid wordt geboden. Deze maatregelen worden op drie functionele gebieden aangeboden door de afdelingen POJZ, I&A en FAC, uitgewerkt in catalogi met standaard diensten (zie bijlage 1 voor schema samenhang beleidsproducten).
5. Maatregelen zijn **in balans** met de te beschermen waarde; dit betekent dat onderzoek gedaan moet worden naar de noodzaak van maatregelen. De Provincie Zeeland gebruikt hiervoor **risicoanalyse**. Risicomanagement is onderdeel van de besluitvorming, zowel bij projecten als bij zaken als procesontwerp, aanschaf van apparatuur en software.
6. **Informatie is intern vrij beschikbaar** voor medewerkers, tenzij de beveiligingsclassificatie van deze informatie anders voorschrijft. Het verantwoordelijk lijnmanagement geeft op basis van de beveiligingsclassificatie van de informatie medewerkers autorisatie voor fysieke en logische toegang.
7. Informatieveiligheid wordt ook meegenomen bij het opzetten en uitvoeren van **(keten)samenwerking**. Ook hierbij wordt risicomanagement toegepast.
8. Er wordt planmatig gewerkt aan het verhogen en borgen van **bewustwording en kennis** van alle medewerkers op het gebied van informatieveiligheid en privacy. Er worden structureel middelen ter beschikking gesteld voor opleiding, communicatie en training. Trainingen m.b.t. de beginselen van veilig werken bij de provincie Zeeland zijn verplicht voor management en medewerkers.

Daar waar afgeweken wordt van een vastgesteld beleid of standaarden, legt het management of de proceseigenaar dit vast in een formele verklaring (‘comply or explain’). De verklaring bevat een risico-inschatting van de afwijking en de mogelijke consequenties en wordt aan de CISO gerapporteerd. Afwijkingen zijn alleen toegestaan na uitvoering van een risicoanalyse en met schriftelijke toestemming van de bestuurder.

3.2. Risico-gebaseerde benadering van informatieveiligheid

De Provincie Zeeland definieert veilig omgaan met informatie als het proces van het beschermen van informatie en gerelateerde componenten (zoals geautomatiseerde informatiesystemen, personen en papieren documenten) tegen onbedoelde of vooropgezette inbreuken van:

- **Beschikbaarheid:** Informatie dient beschikbaar te zijn op het moment dat het nodig is, wat eisen stelt aan de beschikbaarheid van informatiesystemen en databases, ook bij verstoringen.
- **Integriteit:** De gebruiker moet erop kunnen vertrouwen dat informatie juist, volledig, tijdig en geoorloofd is. Handhaving hiervan is verankerd in procesafspraken, maar ook in maatregelen die ongeoorloofde of ongewenste (expres of per ongeluk) mutaties tegengaan.
- **Vertrouwelijkheid:** Gebruikers en belanghebbenden moeten er op kunnen vertrouwen dat informatie alleen beschikbaar is voor die gebruikers die het nodig hebben voor de uitvoering van hun functie en niet onnodig ter inzage van anderen is.
- **Privacy:** Als bijzondere vorm van Vertrouwelijkheid, welke wettelijk is gereguleerd via de AVG: lekken van burgergegevens en/of van klanten raakt direct de reputatie van de Provincie. Lekken van persoonsgegevens roept extra aandacht van de Autoriteit Persoonsgegevens op, die kan dwingen tot kostbare maatregelen en eventueel een boete.

Veilig omgaan met informatie richt zich op de bescherming van informatie tegen bedreigingen en gaat in principe over de beantwoording van drie vragen:

1. Wat zijn onze meest waardevolle gegevens en informatiesystemen?
2. Welke gebeurtenissen kunnen schade toebrengen aan deze gegevens en informatiesystemen?
3. Wat gaan we wel en niet doen om gegevens en informatiesystemen beschermen tegen deze gebeurtenissen?

De Provincie hanteert hierbij een risico-gebaseerde benadering, waarbij op basis van een risicoanalyse maatregelen worden getroffen. Zowel zakelijke overwegingen (kosten en baten) als externe verplichtingen worden in deze benadering meegenomen. Maatregelen staan steeds in verhouding tot de bedrijfsprocessen van de Provincie en de eisen aan de continuïteit hiervan. Eventuele restrisico's worden expliciet door de organisatie geaccepteerd.

4. Organisatie van Informatieveiligheid

4.1. Taken, verantwoordelijkheden en bevoegdheden

Informatieveiligheid is op vier niveaus ingericht en geborgd, waarbij elk niveau een eigen verantwoordelijkheid heeft.

Niveau		
Besturend	Bepalen van de ambitie en het beleid Invullen randvoorwaarden voor invoering van het beleid	Gedeputeerde Staten/ Directie
Coördinerend	Overzicht houden op voortgang invoering en ontwikkeling van beleid en richtlijnen	CIO/CISO
Handhavend	Uitvoering en handhaving van beleid en richtlijnen Herkennen en bewaken van de risico's	CISO/ Lijnmanagement
Uitvoerend	Uitvoering van beleid en richtlijnen	Medewerkers/ Lijn management

Onderstaande opsomming beschrijft de diverse partijen en rollen.

- *Gedeputeerde Staten (GS)*
  GS stellen het informatieveiligheidsbeleid vast. GS zijn het hoogste strategische besluitvormend gremium voor Informatieveiligheid en privacy. De Provincie kent een collectieve bestuurlijke verantwoordelijkheid. GS maken in het kader van de Planning & Control-cyclus afspraken met de aan hen rapporterende managers over de uitvoering van het informatieveiligheidsbeleid en het toezicht hierop en stelt de noodzakelijke middelen beschikbaar.

- *De directie*
  De directie is strategisch eindverantwoordelijk voor de borging van informatieveiligheid van de organisatie en beoordeelt jaarlijks de effectiviteit door middel van de directiebeoordeling. De directie legt de verbinding met het bestuur bij calamiteiten.

- De Chief Information Officer (CIO)
  Het afdelingshoofd Informatie en Automatisering vervult tevens de rol van CIO. Vanuit deze rol adviseert de CIO bestuurders, directie en lijnmanagers over de strategie en tactiek rond informatieveiligheid en zorgt voor de noodzakelijke middelen. De CIO houdt toezicht op de uitvoering en implementatie van het beleid voor informatieveiligheid en is verantwoordelijk voor het functioneren van het managementproces rond informatieveiligheid (PDCA-cyclus). De CIO is verantwoordelijk voor acceptatie van rest risico's.

- *De Chief Information Security Officer (CISO)*
  De CISO rapporteert aan de CIO. Hij coördineert en bewaakt de uitvoering en kwaliteit van het managementproces rond informatieveiligheid (PDCA-cyclus). De CISO ontwikkelt, in samenwerking met de CIO Office en de uitvoerende organisatieonderdelen, operationele richtlijnen en procedures voor informatieveiligheid en continue verbetering. De CISO coördineert en bewaakt de uitvoering van het informatieveiligheidsbeleid en verhoogt en houdt het bewustzijn rond informatieveiligheid op peil door het opstellen en uitvoeren van een bewustwordingsplan. De CISO ondersteunt de organisatie met gevraagd en ongevraagd advies.

- *De functionaris gegevensbescherming (FG)*
  De FG houdt onafhankelijk toezicht op de naleving van de AVG door de Provincie. Daarnaast geeft hij gevraagd en ongevraagd advies over onderwerpen en kwesties die de privacy rechten raken van inwoners of de medewerkers van de provincie. De FG coördineert en bewaakt de uitvoering van het privacybeleid en de protocollen voor gegevensverwerking en datalekken. Samen met de CISO houdt de FG de bewustwording onder collega's op peil om te handelen volgens de AVG-principes en informatieveiligheid. De FG wordt ondersteund door de werkgroep AVG.

- *De Provinciearchivaris*
  De Provinciearchivaris heeft onafhankelijk toezicht op het niet overgebrachte deel en vanuit die hoedanigheid houdt hij ook toezicht op de informatieveiligheid. Hij rapporteert schriftelijk de bevindingen

en aanbevelingen eens per twee jaar rechtstreeks aan de colleges van GS en PS.

- *Het lijnmanagement*
  Het management is eindverantwoordelijk voor informatieveiligheid binnen zijn/haar organisatieonderdeel (afdelingen, opgave of programma). De belangrijkste taak is om in de dagelijkse praktijk toe te zien op de naleving van het beleid en de gemaakte afspraken rond informatieveiligheid door de medewerkers. Daarnaast houdt het management in het oog welke risico's bestaan en ontstaan en hoe daarvoor praktische maatregelen voor te treffen. Het management werkt daarbij nauw samen met de applicatie- en proceseigenaren.

- *De informatiesysteem- en proceseigenaren*
  De informatiesysteem- en proceseigenaren zijn verantwoordelijk voor het uitvoeren van risicoanalyses op processen en onderliggende applicaties en informatiesystemen, zorgen voor vaststelling van bijbehorende beveiligingsmaatregelen en acceptatie van restrisico's. Daarnaast zorgen zij ervoor dat de digitale informatie wordt geclassificeerd conform de gehanteerde classificatiemethodiek en dat de naleving van de relevante maatregelen wordt getoetst. Ze worden hierbij gefaciliteerd door de CISO, de architecten, de werkgroepleden informatiebeveiliging, de Provincieadvocaat, functioneel applicatiebeheerders en key users.

- *De medewerkers*
  Alle medewerkers (inclusief uitzendkrachten, stagiaires etc.) van de Provincie zijn zich bewust van het beleid en de onderliggend richtlijnen en procedures en handelen daarnaar. Hierin worden zij gestuurd door hun leidinggevenden en geadviseerd door de projectgroep informatieveiligheid en de CISO. Bij (noodzakelijke) registratie van tot personen herleidbare gegevens moet worden voldaan aan de AVG. In de jaargesprekken is aandacht voor informatieveiligheid.

- *Externe partijen*
  Alle externe partijen die worden ingehuurd, bijvoorbeeld voor ICT-werkzaamheden, beveiliging en consultants zijn gehouden aan het informatieveiligheidsbeleid. Op basis van een risicoanalyse dienen adequate maatregelen te worden genomen om geheimhouding van informatie zo goed mogelijk te borgen.

4.2. Overleg- en rapportagestructuren informatieveiligheid

De CISO rapporteert en geeft gevraagd en ongevraagd advies aan de CIO, directie en (de portefeuillehouder binnen) GS.

Overleg		
Portefeuillehouder GS – CIO & CISO	Viermaal per jaar en officieus ad hoc	Alleen indien gewenst
CIO – CISO	Maandelijks	Mondeling (ISMS)
Directie – CISO (directiebeoordeling)	Jaarlijks officieel en officieus ad hoc	Directiebeoordeling
CISO – staf IA	Tweewekelijks	Mondeling
Centraal Informatiebeveiligingsoverleg (CIBO) Alle CISO's provincies en BIJ12	Tweewekelijks en ad hoc per mail en app	Notulen en actielijst (ISMS)
Interprovinciaal Information Sharing Analysis Center	Tweemaandelijks waarvan 4 overleggen online en 2 fysiek	Notulen en actielijst
Zeeuwse CISO-kring	Tweemaal per jaar fysiek	Verslag

De rapportage van de CISO volgt verder het stramien van de P&C cyclus en de kwartaalrapportages.

4.3. Relevante contacten

De provincie onderhoudt diverse contacten met overheidsinstanties en belangengroepen. Dit contact kan diverse vormen hebben, van deelname aan werkgroepen, sectorale vergaderingen, netwerkbijeenkomsten. In onderstaande tabel zijn de belangrijkste contacten opgesomd.

Contact	Deelnemer
CIBO overleg (interprovinciaal CISO overleg)	CISO
ICO werkgroep (Inkoopeisen Cyberscurity Overheden)	CISO
Contacten rond security incidenten (NCSC, etc)	CISO
Samenwerkingsverband SSS (Slimmer, Samen Sterker) met BIJ12 en 5 provincies (Groningen, Flevoland, Gelderland, Noord-Brabant, Zeeland)	CISO
Autoriteit Persoonsgegevens	FG
Landelijke werkgroep Digitale Veiligheid	CISO
Strategisch Informatie Overleg (SIO)	CIO
Provinciale Projectgroep Architecten (PPA)	Architecten
Provinciale Overleggroep Functionarissen Gegevensbescherming (POFG)	FG
Interprovinciale Digitale Agenda	Div. IA-leden
Interprovinciaal Information Sharing Analysis Center (IP-ISAC)	CISO (voorzitter) Sr. Adv. Innovatie en Beveilging
Zeeuwse CISO-kring	CISO

5. Naleving en evaluatie

Veiligheidsmaatregelen worden getroffen om risico's te verminderen. Om de controle over de risico's te waarborgen is het noodzakelijk regelmatig na te gaan of maatregelen nog werken en nog steeds de beoogde veiligheid bieden.

De afdeling IA test periodiek de disaster recovery maatregelen en oefent het continuïteitsplan.

Jaarlijks wordt een penetratietest op de systemen uitgevoerd door een onafhankelijke partij en tevens vindt jaarlijks een mystery guest bezoek plaats.

Naast de dagelijkse interne controle door de lijnorganisatie en bewaking door de CISO, voert de afdeling Control interne audits uit. Daar waar het onderwerp van audit specifieke kennis vraagt, huurt de Provincie externe capaciteit in.

De Provincie Zeeland is inmiddels ISO-27001 gecertificeerd zijn. Elke jaar zal een opvolgingsaudit uitgevoerd worden en eens per 3 jaar een hercertificeringsaudit.

Daarnaast vinden periodiek externe, onafhankelijke audits periodiek plaats door de accountant. Bevindingen op het gebied van informatieveiligheid worden afgestemd met en bewaakt door de CISO.

Bijlage 1: Samenhang informatieveiligheidsbeleid met i-beleid provincie